VELEUČLIŠTE NIKOLA TESLA U GOSPĆU

Anđela Tomić

Elektronički potpis i njegova uporaba u Republici Hrvatskoj

Electronic Signature andits Use in Republic of Croatia

Završni rad

Gospić, 2017.

VELEUČILIŠTE NIKOLA TESLA

UPRAVNI ODJEL

PREDDIPLOMSKI STRUČNI UPRAVNI STUDIJ

Elektronički potpis i njegova uporaba u Republici Hrvatskoj

Electronic Signature andits Use in Republic of Croatia

Završni rad

Mentor :

Dr.sc. Katerina Dulčić

Student :

Anđela Tomić

JMBAG: 2963000317/12

Gospić, rujan 2017

Veleučilište „Nikola Tesla“ u Gospiću

Upravni odjel

Gospić, 8. ožujka 2016.

ZADATAK

za završni rad

Pristupnici ***Anđela Tomić*** MBS: 2963000317/12

Studentu stručnog studija Upravnog prava izdaje se tema završnog rada pod nazivom

Elektronički potpis i njegova uporaba u Republici Hrvatskoj

(*Electronic Signature and its Use in Republic of Croatia*)

Sadržaj zadatka :

Pristupnica u izlaganju svoje teme mora poći od definicije elektroničkog potpisa i naprednog elektroničkog potpisa. Kako je pravna regulativa u pogledu elektroničke isprave i elektroničkog potpisa u Hrvatsku uvedenu u pogledu usklađivanja s pravnom tečevinom Europske Unije, neophodno je razmotriti i predmetne smjernice EU, ali i druge međunarodne akte UN-a i UNCITRAL-a, jer primarna svrha elektroničke isprave je komunikacija putem interneta, pa mora imati i međunarodni značaj. Potrebno je razmotriti i izložiti hrvatsku pravnu regulativu kako zakonske akte, tako i podzakonske, te se posebno osvrnuti na limite uporabe elektroničkog potpisa i mogućnosti njegove primjene u državnoj upravi.

Završni rad izraditi sukladno odredbama Pravilnika o završnom radu Veleučilišta „Nikola Tesla“ u Gospiću.

Mentor: mr. sc. Katerina Dulčić, predavač zadano: 3. ožujka 2016. godine , _____
(ime i prezime) (nadnevak) potpis

Pročelnik odjela: dr. sc. Aleksandar Skendžić, v. predavač predati do: _____ , _____
(ime i prezime) (nadnevak) potpis

Student: Anđela Tomić primio zadatak: 9.03.2016. , Anđela Tomić
(ime i prezime) (nadnevak) potpis

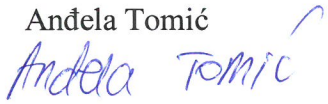
Dostavlja se:

- mentoru
- pristupniku

I Z J A V A

Izjavljujem da sam završni rad pod naslovom Elektronički potpis i njegova uporaba u Republici Hrvatskoj izradila samostalno pod nadzorom i uz stručnu pomoć mentorice prof.dr.sc. Katerine Dulčić

Anđela Tomić



SAŽETAK

Na sljedećim stranicama ovog završnog rada autorica je obradila temu o elektroničkom potpisu i ukazala na, nazovimo ga, novi i pojednostavljeni način rada uprave te na postignutu novu razinu sigurnosti kako rada tako i zaštite podataka.

Na samom početku nije samo definiran pojam elektroničkog potpisa već se također dotiče načina na koji taj potpis funkcionira te koja mu je uopće svrha.

Riješivši temeljna pitanja o tome što je elektronički potpis, njegova svrha i način rada autorica se posvetila razradi teme, točnije o tome kako se i kojim zakonskim aktima uređuju norme o elektroničkom potpisu kako na području Republike Hrvatske i na području Europske Unije.

Ključne riječi: elektronički potpis, zakonski akti

SUMMARY

On the following pages of this final work,author elaboratedthe topic of electronic signature and pointed out, let's call it, the new and simplified way of working of public administration and about efficiency, and also of a new level of security of work and data protection.

At theverybeginningofthispaperwork,the author didnotjustdefinethetermofelectronic signature, she also hasbriefly explainedthewaysinwhichthat signature worksandwhatisitspurposeafterall.

Having solved the fundamental questions about what an electronic signature is, its purpose, and the way it works,the authorfurther developedher research, specifically, about how it is legally regulated and what legal acts regulate the standards of the electronic signature, both on the territory of the Republic of Croatia and in the territory of the European Union.

Keywords: electronic signature, legal act

SADRŽAJ

UVOD

Danas je elektronička komunikacija prisutna gotovo svugdje. U poslovnoj komunikaciji elektronička pošta gotovo je zamijenila klasičnu poštu na papiru. Elektronička komunikacija danas predstavlja nezamjenjiv način komunikacije između poslovnih partnera.

Elektronički potpis ključan je element uspjeha elektroničke trgovine, te je zapravo uvjet kako elektronička trgovina ne bi bila nepouzdana i nesigurna. Današnje tehnologije koje poznajemo ne pružaju nužno apsolutnu sigurnost , ali omogućuju nužnu razinu zaštite koja je usporediva, ako ne i bolja od papirnate komunikacije.

Predaja i preuzimanje dokumenata i obrazaca, pristup poslovnim informacijama, e-plaćanje, razmjena elektroničkih računa i elektroničko potpisivanje dokumenata samo su neke od pogodnosti koje su dostupne putem interneta. Uz sve prednosti koje donosi, bez napredne elektroničke zaštite i platforme povjerenja, elektroničko poslovanje može biti i izvor brojnih rizika.

Da bi elektronički dokument bio prihvaćen, mora se temeljiti na prihvaćanju tehničke ispravnosti dokumenta, nepromjenjivosti sadržaja i vjerodostojnosti izvora, odnosno stvaratelja dokumenta. Sve se to može jedinstveno obuhvatiti instrumentom koji osigurava vjerodostojnost izvora i zaštitu integriteta sadržaja, a to je elektronički potpis.[1]

[1] FINA WEB, primjena certifikata, Elektronički potpis http://www.fina.hr/Default.aspx?art=10737

1. Elektronički potpis

1.1. Pojam Elektroničkog potpisa

Predstavlja generički pojam koji podrazumijeva čitav niz različitih vrsta digitalno prikazanih podataka pomoću kojih se vrši identifikacija korisnika i provjera vjerodostojnosti potpisanog elektroničkog dokumenata.

Dodatna vrijednost potpisanog elektroničkog dokumenta postiže se primjenom naprednog elektroničkog potpisa.

Po članku 3 ZAKONA O ELEKTRONIČKOM POTPISU (NN 10/02,80/08, 30/14)elektroničkog potpisa, koju je izglasao Hrvatski Sabor elektronički potpis je: „Elektronički potpis u smislu ovoga Zakona je skup podataka u elektroničkom obliku koji služe za identifikaciju potpisnika i potvrdu vjerodostojnosti potpisanoga elektroničkog zapisa."

Elektronički potpis podrazumijeva skup podataka u elektroničkom obliku pomoću kojih se vrši identifikacija potpisnika i provjera vjerodostojnosti potpisanog elektroničkog dokumenta.

Elektronički potpis je niz znakova u elektroničkom obliku. Kreiran računalom i ima istu pravnu snagu kao i vlastoručni potpis.

Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća, od 23. srpnja 2014., o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, Službeni list Europske unije, br. 257/14 od 2014. čl. 3. st. 1. t. 10. „„elektronički potpis" znači podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje;"

Pitanje definicije potpisa osobito je važno u vremenu kada intenzivno prelazimo na komunikaciju putem elektroničkih informacijskih sustava. Broj elektroničkih dokumenata u državnoj upravi, pravosuđu i gospodarstvu u stalnom je porastu. Kako informacijska tehnologija napreduje, tako se šire i mogućnost i njezine upotrebe. Budući da upotreba elektroničkih informacijskih sustava u društvu u cjelini raste, gospodarski subjekti i državna

uprava, žele li (p)ostati efikasni, trebaju prihvatiti i upotrebljavati moderne informacijske tehnologije poput elektroničkog potpisa u svakodnevnom radu.[2]

1.2. Napredni elektronički potpis

Napredni elektronički potpis ima istu pravnu snagu kao vlastoručni potpis i otisak pečata na papiru, ako je izrađen u skladu s odredbama Zakona o elektroničkom potpisu, a povezan je isključivo s potpisnikom te ga nedvojbeno identificira. Prema uredbi Zakona o elektroničkom potpisu od strane Europske unije članak bi bio van snage, jer uredba ujedno definira i elektronički pečat. Po EU „napredan elektronički pečat" znači elektronički pečat koji ispunjava zahtjev navedene u članku 36.;

Elektronički potpis osigurava autorizaciju pošiljatelja, provjeru da li je poruka mijenjana u prijenosu i neporecivost poslane poruke.

Elektroničkim potpisom osigurava se:

a) AUTENTIČNOST – osigurava da je pošiljatelj stvarno onaj koji tvrdi da on jest

b) INTEGRITET – jamči cjelovitost i nepromijenjenost poruke

Dodatna vrijednost potpisanog elektroničkog dokumenta postiže se korištenjem naprednog elektroničkog potpisa. Ukoliko je izrađen u skladu sa odredbama Zakona o elektroničkom potpisu, ima istu pravnu snagu i zamjenjuje vlastoručni potpis, odnosno vlastoručni potpis i otisak pečata na elektroničkom dokumentu. Njegovim korištenjem uz autentičnost i integritet osigurava se i neporecivost dokumenta, a to znači da pošiljatelj ne može opovrgnuti odnosno poreći potpisanu transakciju.

Zakon o naprednom elektroničkom potpisu:

"Napredan elektronički potpis ima istu pravnu snagu i zamjenjuje vlastoručni potpis, odnosno vlastoručni potpis i otisak pečata ako je izrađen u skladu s odredbama ovoga Zakona, te ako su ispunjeni ostali uvjeti propisani ovim Zakonom i propisima koji su donijeti na temelju

[2] Tihomir Katulić, razvoj pravne regulacije elektroničkog potpisa, elektroničkog certifikata i elektroničke isprave u Hrvatskom i poredbenom pravu, Zbornik pravnog fakulteta u Zagrebu 2011, str.1342.

ovoga Zakona." – Čl 5; zakona o eletroničkom potpisu.

Također, u zakonu napredni elektronički potpisa elektronički potpis je:

1. je povezan isključivo s potpisnikom,

2. nedvojbeno identificira potpisnika,

3. nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika,

4. sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka.[3]

Uvjeti koji se postavljaju pred napredni elektronički potpis prilično su strogi, no nužni ako je cilj njime zamijeniti tradicionalni potpis na papiru. Naravno, kao što je i ručni potpis na papiru tehnički moguće krivotvoriti sa svim posljedicama koje to predstavlja za pravnu sigurnost, isto se može reći i za napredni elektronički potpis. Međutim, uvjeti koje zakonodavac propisuje u najvećoj mogućoj mjeri osiguravaju dokumente i komunikaciju potpisanu naprednim elektroničkim potpisom od zloporabe.

Po čl. 26 i 36. Zakona o elektroničkom potpisu napredan elektronički potpis mora sadržavati:

(a) na nedvojben način je povezan s potpisnikom;

(b) omogućava identificiranje potpisnika;

(c) izrađen je korištenjem podacima za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom; i

(d) povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.

1.3. Tehnologije elektroničkog potpisa

Postoji više načina da čovjek ostavi svoj jedinstveni potpis kojim ga možemo identificirati, a najpoznatiji načini su:

- Skenirani ručni potpis
- Biometrijski potpis (Biometrics Signature Verification)

[3] Zakon o elektroničkom potpisu NN 10/02,80,/08,30/14, zakon je van snage, svi vezani akti su na snazi, čl.4

- Digitalni potpis (kriptografija javnog ključa)

Skenirani ručni potpis je digitaliziran ručni potpis u seriju bitova i upisan u datoteku potpisa, potpis se provjerava usporedbom primljenog potpisa sa onim iz datoteke, mijenjanje dokumenta nema utjecaja na izgled potpisa.

Biometrijski potpis koristi dijelove tijela za identifikaciju (DNK, mrežnica oka, obrazi, govor, ruke, otisak prsta), karakteristike dijelova tijela se pohranjuju u datoteku radi identifikacije. Primjenu nalazi kod kreditnih kartica, sigurnosnih bedževa i kod ulaza u kontrolirane prostore.

2. Način funkcioniranja elektroničkog potpisa

Elektronički potpis je kombinacija dvije kriptografske metode – HASH funkcije koja se koristi za utvrđivanje integriteta poruke i asimetričnog algoritma enkripcije (poput poznatoga RSA algoritma) kojom se najprije izračunava HASH vrijednost poruke (MD5, SHA1...), a zatim se ta vrijednost šifrira ključem potpisnika.

Zajedno sa certifikatom autentičnosti koji je izdan od kvalificiranog agenta koristi se za utvrđivanje vjerodostojnosti potpisa. Potrebno je da primatelj javnim ključem potpisnika dešifrira HASH i zatim ga usporedi sa primljenom porukom. Ako bilo koji element potpisa ili poruke ne odgovara doći će do otkrivanja problema.

2.1. Pojam kriptografije

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda slanja poruka u takvom obliku da ih može pročitati samo onaj kome su namijenjene. Sama riječ kriptografija je grčkog podrijetla i znači tajnopis.[4] Za razliku od dešifriranja, kriptoanaliza ili dekriptiranje je znanstvena disciplina koja se bavi proučavanjem postupaka čitanja skrivenih poruka bez poznavanja ključa. Kriptologija je grana znanosti koja obuhvaća kriptografiju i kriptoanalizu.

2.2. Izrada elektroničkog potpisa

Napredni Elektronički potpis se izrađuje na osnovu tajnog ključa pošiljatelja i samog sadržaja, te se obično ugrađuje u sam sadržaj ili se šalje kao zasebna informacija uz pripadajući sadržaj. Da bi primatelj sadržaja mogao provjeriti elektronički potpis, uz sadržaj i signaturu potrebna mu je i informacija javnog ključa pošiljatelja koju obično pribavi iz drugog, nezavisnog izvora, a ne iz same poruke. Kada bi pribavili informaciju javnog ključa iz elektroničkog potpisa, sama autentičnost izvornosti javnog ključa imala bi smisla samo ako bismo informaciju javnog ključa mogli provjeriti na neki drugi način.

2.3. Protokol šifrirane i potpisane poruke:

1. Sudionik A odabire simetrični ključ K (npr. pomoću generatora slučajnih brojeva) i s pomoću njega šifrira DES postupkom jasni tekst informacije koji želi poslati sudioniku

[4] Andrej Dujella, Marcel Maretić, Kriptografija, Element Zagreb 2007, str.3

B, a time je određen sadržaj digitalne omotnice

2. Iz izvornog sadržaja informacije sudionik A izračunava sažetak S

3. Nakon toga sudionik A svojim tajnim ključem K (koji zna samo on) šifrira odabrani simetrični ključ K i sažetak S, i on šifrirani tekst E (K, S, K) kao zapečaćenu omotnicu pridodaje sadržaju omotnice

4. Po primitku zapečaćene omotnice, sudionik B je otvara tako da javni ključem KEA doznaje simetrični ključ K i sažetak S

5. Poslije toga sudionik B dobivenim simetričnim ključem K dešifrira sadržaj omotnice i tako dolazi do informacije koja mu je poslana

6. Iz dešifriranog sadržaja informacije sudionik B izračunava sažetak i uspoređuje ga s dešifriranim primljenim sažetkom S, i ako su te dvije vrijednosti jednake, smatra primljenu informaciju vjerodostojnom ili besprijekornom, a pošiljatelja poruke autentičnim. [5]

[5]Ledinski,Stjepan, Sustavna progrmska potpora,Varaždin 2003
https://webcache.googleusercontent.com/search?q=cache:ApBD0sh0vekJ:https://documents.tips/documents/elektronicki-potpis.html+&cd=1&hl=hr&ct=clnk&gl=hr

3. Elektronski mediji

Elektronski mediji, a posebno razmjena podataka preko mreže postaju neizostavni u našem privatnom i poslovnom životu. Podatke preko mreže razmjenjujemo sa osobama koje ne poznajemo i u koje samim time ne možemo imati povjerenja, kao ni u to da nam poslani podaci stižu u nepromijenjenom obliku.

Tehnika elektroničkog potpisa predstavlja rješenje ovih problema jer omogućava da se sa pravnom sigurnošću utvrdi tko je poslao elektronsku poruku i da li su podaci u toku svog puta mijenjani. U takvim uvjetima postavlja se pitanje kako osigurati vjerodostojnost komunikacije. Jedan od odgovara na ovo pitanje upravo je institut „elektroničkog potpisa“, koji ukoliko se koristi u zakonom određenim uvjetima, zamjenjuje tradicionalni potpis na papiru. Prije svega, kada govorimo o elektroničkim potpisima treba uzeti u obzir da se, sukladno Direktivi EC/1999/93, istim može potpisati samo i isključivo elektronički dokument, dakle, iz navedenog bi proizlazilo da se tradicionalni dokument-papirnati, ne može kombinirati s e-potpisom.

3.1. Sredstva za elektronički potpis

Sredstvo za elektronički potpis čine računalna oprema, računalni program ili njihove relevantni sastojci koji su namijenjeni za primjenu od strane davatelja usluga certificiranja za, davatelja usluga u vezi s elektroničkim potpisom ili su namijenjeni za primjenu kod izrade ili verificiranja elektroničkih potpisa.

Sredstvo za verificiranje potpisa označava odgovarajuću računalnu opremu ili računalni program koji se koristi za primjenu podataka za verificiranje potpisa.

Verifikacija je proces ispitivanja poruke ili integriteta elektroničkog potpisa izvođenjem HASH funkcije na strani pošiljatelja i primatelja poruke i uspoređivanje rezultata.[6]

[6] Ledinski,Stjepan,Sustavna programska potpora, Varždin 2003
https://webcache.googleusercontent.com/search?q=cache:ApBD0sh0vekJ:https://documents.tips/documents/elektronicki-potpis.html+&cd=1&hl=hr&ct=clnk&gl=hr

4. Vremenski žig

Originalna inačica Zakona o elektroničkom potpisu iz 2002. godine čl. 2 nije uključivala definiciju vremenskog žiga. Izmjenama i dopunama iz 2008. pojam "vremenski žig" uveden je za oznaku digitalnog vremenskog biljega u čl. 1

Vremenski žig, odnosno digitalni vremenski biljeg metoda je označavanja nastanka elektroničkog dokumenta i bilježenja promjena njegova sadržaja kroz vrijeme, odnosno riječ je o mehanizmu provjere kada je digitalni dokument kreiran, odnosno promijenjen, što je važno za utvrđivanje vjerodostojnosti dokumenata.

Po Uredbi EU 910/2014 od 23.srpnja 2014 g. Elektronički vremenski žig" označava podatke u elektroničkom obliku koji povezuju druge podatke u elektroničkom obliku s određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme.

Financijska Agencija (Fina) je trenutno jedini evidentirani izdavatelj vremenskog žiga u Republici Hrvatskoj. Omogućuje pouzdano dokazivanje da je podatak, elektronički zapis, elektronički dokument i sl. postojao prije trenutka u vremenu koji je naznačen u vremenskom žigu. Svaka naknadna promjena u dokumentu i u ugrađenom vremenskom žigu se lako otkriva.

Vremenski žig osigurava sljedeće:

- da je dokument u tom obliku postojao prije vremena navedenog u ugrađenom vremenskom žigu,
- da dokument nije mijenjan nakon vremena navedenog u ugrađenom vremenskom žigu,
- da se verifikacija elektroničkog potpisa dokumenta može pouzdano obaviti i nakon opoziva ili isteka potpisnog certifikata, da je dokument poslan ili zaprimljen u vrijeme navedeno u vremenskom žigu i sl.Zakonodavac u točki 3 prvog stavka čl. 2 Zakona definira pojam i ulogu vremenskog žiga kao elektronički potpisanu potvrdu izdavatelja koja potvrđuje sadržaj podataka na koje se odnosi u navedenu vremenu.

5. Elektronički pečat prema EU uredbi

Prema EU odredbi elektronički su podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje.

Po istim odredbama EU potpisnik je fizička osoba koja izrađuje navedeni potpis, uz jedinstvene podatke potrebne za izradu elektroničkog potpisa. Podaci moraju imati certifikat tj. elektroničku potvrdu koja povezuje podatke za validaciju elektroničkog potpisa s fizičkom osobom i potvrđuje barem ime ili pseudonim te osobe

Uredbe EU određuju i određene definicije u kojima se „autor pečata" definira kao pravna osoba koja izrađuje elektronički pečat, dok „elektronički pečat" definira kao podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka.

6. Certifikat

Certifikat je elektronička identifikacija sudionika u mreži, identificira računalo, osobu, poduzeće, certifikatora na mreži uz poruku, i pošiljatelj dostavlja svoj elektronički potpis. Pomoću certifikata primatelj identificira pošiljatelja i to na način da dešifrira poruku javnim ključem pošiljatelja i provjeri u bazi certifikata.

Certifikat- znači potvrdu u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom i potvrđuje identitet te osobe.

Usluga certificiranja označava pravnu ili fizičku osobu koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima. Digitalna omotnica osigurava tajnost, ali ne i besprijekornost informacije. Digitalni pečat je digitalno potpisana digitalna omotnica.

Certifikat se također koristi za potvrdu identiteta, označava potvrdu u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa (javni ključ) s nekom osobom i potvrđuje identitet te osobe. Napredni elektronički potpis temelji se na kvalificiranom certifikatu.

6.1. Kvalificirani certifikat

To je, elektronička potvrda kojom davatelj usluga izdavanja kvalificiranih certifikata potvrđuje napredni elektronički potpis potpisnika tj. nedvojbeno potvrđuje identitet potpisnika.

Po čl. 10 Zakona o elektroničkom potpisu certifikat je: „Certifikat je, u smislu ovoga Zakona, svaka elektronička potvrda kojom se potvrđuje identitet potpisnika u postupcima razmjene elektroničkih zapisa."

Također, kada bi tumačili zakon certifikat po zakonu mora sadržavati:

1. oznaku o tome da se radi o kvalificiranom certifikatu,

2. identifikacijski skup podataka o osobi koja izdaje certifikat (osobno ime; ime oca ili majke; nadimak, ako ga osoba ima; datum rođenja; prebivalište, odnosno boravište; naziv pravne osobe i sjedište, ako certifikat izdaje pravna osoba),

3. identifikacijski skup podataka o potpisniku (osobno ime, ime oca ili majke, nadimak, ako ga osoba ima, datum rođenja, prebivalište, odnosno boravište).

4. podatke za verificiranje elektroničkog potpisa koji odgovaraju podacima za izradu

elektroničkog potpisa koji su pod kontrolom potpisnika,

5. podatke o početku i kraju važenja certifikata,

6. identifikacijsku oznaku izdanog certifikata (brojčanu ili drugu oznaku, te datum izdavanja),

7. napredni elektronički potpis davatelja usluge izdavanja kvalificiranih certifikata,

8. ograničenja vezana za uporabu certifikata, ako ih ima,

9. ograničenja na vrijednost poslovnih događaja za koje se daje certifikat, ako ih ima.

Davatelj usluga izdavanja kvalificiranih certifikata dužan je osigurati rizik od odgovornosti za štete koje nastanu obavljanjem usluga certificiranja (obvezno osiguranje). Ministar gospodarstva pravilnikom utvrđuje najniži iznos osiguranja iz stavka 3. članka.

7. Primjena elektroničkog potpisa

Elektronički potpis ima široku primjenu u elektroničkoj razmjeni podataka. Neki od primjera su: korištenje e-potpisa za potpisivanja poruka elektroničke pošte, potpisivanje dokumenata u pdf formatu…

Elektronički potpis koristi se za:

1. potvrdu identiteta pošiljatelja elektronički potpisanog dokumenta
2. provjeru integriteta sadržaja dokumenta (tj. provjeravanje da originalni sadržaj dokumenta nije bio izmijenjen prilikom prijenosa).[7]

7.1. Potpisnik elektroničkog potpisa

Potpisnik elektroničkog potpisa je osoba koja posjeduje sredstvo za izradu elektroničkog potpisa koji potpisuje. Navedena osoba djeluje u svoje ime ili u ime fizičke ili pravne osobe koju predstavlja. Navedenim potpisom može se služiti svaka fizička osoba u vlastito ime, kao i osobe koje imaju pravo zastupanja pravnih osoba ili ako imaju pravo nad zastupanjem drugih fizičkih osoba, također regulirano zakonom.

7.2. Svrha Elektroničkog potpisa

7.2.1. Elektroničko bankarstvo

Bankarske transakcije (uplate, isplate i ostalo) obavljaju se elektroničkim putem bez prisutnosti bankarskih službenika.

Donosi brojne pogodnosti bržim i jednostavnijim pristupom računima i financijskim sredstvima. Nakon e-trgovine to je najrazvijeniji segment elektroničkog poslovanja.

7.2.2. Elektroničko poslovanje

Elektroničko poslovanje je oblik rada u razmjeni strukturiranih i nestrukturiranih poslovnih dokumenata elektronskim putem između poslovnih partnera, a uključuje i elektroničku trgovinu.

[7] MINGO HR, Ministarstvo gospodarstva, e- Potpis, http://www.mingo.hr/page/kategorija/e-potpis

7.3. Način dobivanja elektroničkog potpisa

Kako bi koristili e-potpis potreban Vam je certifikat, sredstvo za izradu elektroničkog potpisa, te odgovarajuća računalna aplikacija.

U Republici Hrvatskoj je za sada jedini ovlašteni izdavatelj certifikata Financijska agencija (FINA) koja izdaje certifikate pravnim i fizičkim osobama te je Uredbom Vlade RH (NN 146/04) određena kao nositelj poslova certificiranja za tijela državne uprave.

Kvalificirani certifikati davatelja usluga certificiranja sa sjedištem u Europskoj uniji jednako su valjani kao i kvalificirani certifikati izdani u Republici Hrvatskoj.

Kvalificirani certifikati davatelja usluga certificiranja sa sjedištem u zemljama izvan Europske unije jednako su valjani kao i kvalificirani certifikati izdani u Republici Hrvatskoj:

1. ako davatelj usluga certificiranja ispunjava uvjete za izdavanje kvalificiranih certifikata iz Zakona o elektroničkom potpisu te je dobrovoljno akreditiran u Republici Hrvatskoj ili jednoj od zemalja članica Europske unije,
2. ako neki domaći davatelj usluga certificiranja koji ispunjava uvjete za izdavanje kvalificiranih certifikata iz Zakona o elektroničkom potpisu jamči za takve certifikate jednako kao da su njegovi,
3. ako tako odredi bilateralni ili multilateralni sporazum između Republike Hrvatske i drugih zemalja ili međunarodnih organizacija,
4. ako tako odredi bilateralni ili multilateralni sporazum između Europske unije i trećih zemalja ili međunarodnih organizacija.

Certifikati davatelja usluga certificiranja sa sjedištem u Europskoj uniji, koje prema zakonu nije moguće odrediti kao kvalificirane, imaju istu pravnu snagu kao i certifikati izdani u Republici Hrvatskoj u skladu s odredbama Zakona o elektroničkom potpisu[8] ali da je prije navedeni propis ne važeći pozvati se treba na Uredbu EU o elektroničkom potpisu

[8] MINGO HR, Ministarstvo Gospodrstva, e-Potpis, http://www.mingo.hr/page/kategorija/e-potpis

Po općim odredbama Zakona o osobnoj iskaznici NN 11/2002, 62/15 , navedena iskaznica je isprava kojom hrvatski državljanin dokazuje identitet, hrvatsko državljanstvo, spol, datum rođenja i prebivalište u Republici Hrvatskoj.

Po čl. 2. Zakona o osobnoj iskaznici:

(1) Osobna iskaznica sadržava elektronički nosač podataka na koji se uz podatke iz članka 1. stavka 1. ovoga Zakona može pohraniti jedan ili dva certifikata.

(2) Certifikati koji se mogu pohraniti na elektronički nosač podataka iz stavka 1. ovoga članka su identifikacijski certifikat i potpisni certifikat.

(3) Identifikacijski certifikat je kvalificirani certifikat koji se koristi za elektroničku identifikaciju i autentifikaciju radi pristupa elektroničkim uslugama.

(4) Potpisni certifikat je kvalificirani certifikat koji se koristi za podršku naprednom elektroničkom potpisu koji ima istu pravnu snagu i zamjenjuje vlastoručni potpis sukladno propisima kojima je reguliran elektronički potpis.

(5) Davatelj usluga certificiranja koji obavlja poslove izdavanja certifikata iz stavaka 3. i 4. ovoga članka je pravna osoba ovlaštena za izradu osobnih iskaznica.

(6) Davatelj usluga certificiranja iz stavka 5. ovoga članka dužan je uspostaviti Portal elektroničke osobne iskaznice na kojem će objavljivati sve informacije potrebne za korištenje osobne iskaznice, donijeti interni akt o postupcima certificiranja te se upisati u evidenciju ministarstva nadležnog za poslove gospodarstva kao davatelj usluga certificiranja koji obavlja usluge izdavanja kvalificiranih certifikata te provesti integraciju u sustav e-Građani sukladno propisima o državnoj informacijskoj infrastrukturi.

7.4. Pouzdanost elektroničkog potpisa

Pouzdani popis predstavlja javno objavljen popis nadziranih i dobrovoljno akreditiranih davatelja usluga izdavanja kvalificiranih certifikata te mora pružati osnovne informacije o istima. Pouzdani potpis treba biti objavljen u strojno čitljivom obliku (XML), a može biti objavljen i u ljudski čitljivom obliku (pdf).

Sigurnost i pouzdanost poslovanja putem interneta jamči najsuvremenija PKI tehnologija koja se temelji na pametnim karticama s digitalnim certifikatima. Korištenje elektroničkog potpisa postaje iznimno važan, siguran i nezamjenjiv vid komunikacije.

IETF definicija PKI sustava glasi: PKI je skup sklopovlja, programske opreme, ljudi, pravila i funkcija potrebnih za stvaranje, upravljanje, pohranjivanje, distribuiranje i opozivanje certifikata baziranih na kriptografiji javnim ključem.

NCARH je nacionalni ovjerovitelj za RH koji omogućuje povezivanje domena povjerenja unutar HR PKI domene.

Povezivanje omogućuje cross certificiranje glavnih ovjerovitelja različitih PKI domena unutar HR PKI domene.

Povjerenstvo za HR PKI postavlja, upravlja i objavljuje politike u domeni HR PKI i upravlja radom NCARH-a i repozitorijom. Odgovoran je za certificiranje i akreditaciju unutar cjelokupne HR PKI domene te ima odgovornost za nadzor svih PKI operacija, te je zaduženo za:

- identifikaciju međunarodnih i europskih normi iz područja PKI i njihovu implementaciju u HR PKI,
- uspostavu, odobravanje i održavanje politike certificiranja za NCARH
- odobravanje operativnih postupaka u HR PKI
- uspostavu i odobravanje prikladnih mehanizama kontrola i izvještajnih procedura za HR PKI,
- prihvaćanje zahtjeva od strane davatelja usluga certificiranja koji se žele udružiti u HR PKI te odobravanje, izdavanje povezujućih certifikata za glavnog ovjerovitelja davatelja usluga certificiranja,
- odobravanje, izdavanje povezujućih certifikata za glavnog ovjerovitelja davatelja usluga certificiranja
- poticanje na suradnju s prekograničnim PKI domenama
- donošenje smjernica za rad i daljnji razvoj NCARH-a. [9]

[9] MINGO HR, Ministarstvo Gospodrstva, e-Potpis, http://www.mingo.hr/page/kategorija/e-potpis

7.5. Nadzor elektroničkog potpisa

Svaki davatelj usluga certificiranja u RH nadziran je od strane ovlaštenog nadležnog tijela u RH. Ministarstvo gospodarstva i Ministarstvo financija u Republici Hrvatskoj, tijela su državne uprave ovlaštena za provođenje inspekcijskog nadzora nad radom davatelja usluga certificiranja.

Davateljima usluga certificiranja nije potrebna posebna dozvola za obavljanje usluga certificiranja, ali su Ministarstvu gospodarstva dužni prijaviti početak obavljanja usluga certificiranja, najmanje osam dana prije početka rada. Uz prijavu i ili u slučajevima promjena u obavljanju usluge, davatelj usluga certificiranja prilaže svoje interne akte o načinu i postupcima pružanja usluga certificiranja te o tehničkoj infrastrukturi.

Davatelji usluga certificiranja koji obavljaju usluge izdavanja kvalificiranih certifikata moraju u svojim internim pravilima uzeti u obzir sigurnosne zahtjeve određene Zakonom o elektroničkom potpisu i pripadajućim pod zakonskim propisima.

Prilikom provođenja nadzora, utvrđuje se jesu li ispunjeni svi uvjeti propisani Zakonom o elektroničkom potpisu i pripadajućim pod zakonskim propisima. Nadzire se pravilnost primjene propisanih postupaka i organizacijsko tehničkih mjera te primjena internih pravila u skladu sa Zakonom o elektroničkom potpisu.

Poslove vezane uz akreditaciju davatelja usluga certificiranja u RH, obavlja Hrvatska akreditacijska agencija.

Davatelji usluga certificiranja koji dokažu da ispunjavaju zakonom propisane uvjete mogu zahtijevati da ih akreditacijsko tijelo upiše u Registar akreditiranih davatelja usluga certificiranja. Akreditirati se mogu i strani davatelji usluga certificiranja ako ispunjavaju zakonom definirane uvjete.

Zakon o elektroničkom potpisu u smjeru nadzora, u čl 36:37 i 38 tumači provođenje nadzora elektroničkog potpisa:

„Članak 36. Inspekcijski nadzor nad radom davatelja usluga certificiranja provode nadležni inspektori Ministarstva gospodarstva i Ministarstva financija. Nadzor nad radom davatelja usluga certificiranja u području prikupljanja, uporabe i zaštite osobnih podataka potpisnika mogu provoditi i državna te druga tijela određena zakonom i drugim propisima koji uređuju

zaštitu osobnih podataka.

Članak 37. U okviru inspekcijskog nadzora Ministarstvo nadzire rad registriranih, odnosno evidentiranih davatelja usluga certificiranja, te:

– utvrđuje jesu li ispunjeni uvjeti propisani ovim Zakonom i provedbenim propisima donesenim na temelju ovoga Zakona,

– nadzire pravilnost primjene propisanih postupaka i organizacijsko-tehničkih mjera te primjenu internih pravila koja su u svezi s uvjetima propisanima ovim Zakonom i provedbenim propisima donesenim na temelju ovoga Zakona.

Ako registrirani, odnosno evidentirani davatelj usluga certificiranja ne ispunjava uvjete propisane ovim Zakonom i provedbenim propisima donesenim na temelju ovoga Zakona, državni službenik Ministarstva ovlašten za provedbu inspekcijskog nadzora donosi rješenje u upravnom postupku kojim se privremeno zabranjuje davanje usluga certificiranja.

Članak 38. Davatelj usluga certificiranja je dužan radi provedbe inspekcijskog nadzora omogućiti državnim službenicima Ministarstva ovlaštenim za provedbu inspekcijskog nadzora neograničen uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru potpisnika i pridruženoj računalnoj opremi i uređajima.

7.6. Neovlašten pristupa certificiranja

Po zakonu će se novčanom kaznom kazniti svi koji neovlašteno izdaju certifikate, ne provode odgovarajuće zaštitne mjere , ne obavještavaju potpisnika o bitnim uvjetima uporabe izdanog certifikata, ne vode ažurno evidenciju i ne ispunjavaju rokove, te se ne pridržavaju Zakona.

Sve te i druge stavke koje mogu dovesti do problema zakonom su od strane Ministarstva regulirane novčanim kaznama, i to od 2000,00 do 10.000,00kn.

Po zakonu stavka 6, i navedenih članaka od 39. do 41. tumači se kažnjavanje neovlaštenog korištenja certificiranja:

“VI. KAZNENE ODREDBE

Članak 39.

Novčanom kaznom od 2.000,00 do 10.000,00 kuna kaznit će se za prekršaj fizička osoba

koja:

– neovlašteno pristupi i uporabi podatke i sredstva za izradu elektroničkog potpisa i naprednoga elektroničkog potpisa.

Članak 40.

Novčanom kaznom od 2.000,00 do 10.000,00 kuna kaznit će se za prekršaj potpisnik, odnosno fizička osoba ili odgovorna osoba pravne osobe koja zastupa potpisnika, a koja:

1. nepažljivo i neodgovorno koristi sredstva i podatke za izradu elektroničkog potpisa (članak 26.),

2. davatelju usluga certificiranja u roku ne dostavi potrebne podatke i informacije o promjenama koje utječu ili mogu utjecati na točnost elektroničkog potpisa (članak 27. stavak 1.),

3. davatelju usluga certificiranja pravodobno ne dostavi zahtjev za opoziv certifikata (članak 27. stavak 2.).

Članak 41.

Novčanom kaznom od 5.000,00 do 100.000,00 kuna kaznit će se za prekršaj davatelj usluga certificiranja koji:

1. izdaje kvalificirani certifikat koji ne sadrži sve potrebne podatke ili sadrži podatke koji nisu predviđeni (članak 11. stavak 2.),

2. ne provodi odgovarajuće zaštitne mjere kojima se onemogućuje neovlašteno pohranjivanje i kopiranje podatka za izradu elektroničkog potpisa (članak 17. stavak 1. točka 10.).

3. ne obavijesti potpisnika kojem izdaje certifikat o svim bitnim uvjetima uporabe izdanog certifikata (članak 17. stavak 1. točka 11.),

4. ne utvrdi pravovaljano identitet fizičke ili pravne osobe za koju izdaje kvalificirani certifikat (članak 29. stavak 1. točka 2.),

5. ne vodi ažurno i sigurnosnim mjerama zaštićenu evidenciju certifikata i ne omogući njihovu javnu dostupnost (članak 29. stavak 1. točka 6.),

6. ne vodi ažurno evidenciju svih opozvanih certifikata (članak 30. stavak 2.),

7. ne obavijesti u propisanom roku potpisnika o izvršenom opozivu certifikata (članak 30. stavak 3.),

8. ne obavijesti u propisanom roku Ministarstvo o izvršenim opozivima certifikata (članak

30. stavak 4.),

9. pravodobno ne obavijesti potpisnike kojima je izdao certifikate i Ministarstvo o mogućem stečaju ili drugim okolnostima koje mogu dovesti do prekida obavljanja usluga certificiranja (članak 33. stavak 1.)." **(10)**

Za neovlašteno certificiranje Zakon je donio kaznene odredbe za sve osobe koje se neovlašteno ponašaju prema certifikatima. Zapravo, zakon kažnjava sve koji se ne pridržavaju Zakona, te mogu na bilo koji način dovesti do zablude ili neovlaštenog ili iskrivljenog tumačenja certificiranja.

7.7. Dokazivanje sadržaja elektronskog potpisa

Dođe li pri ispunjenju ugovora do problema ili sporova, svatko mora, tko se na neki ugovor poziva, ili ga želi pobijati, dokazati sadržaj ugovora, odnosno dokazati razloge pobijanja.

Stoga se postavlja pitanje, na koji način u okviru sudskog postupka mogu biti dokazani ugovori koji se temelje na elektroničkom očitovanju volje.

Polazna točka za pitanje dokazne vrijednosti elektronskog očitovanja volje je stanje stalne mogućnosti mijenjanja web stranica.

Zbog toga ona u elektroničkom obliku – bez osiguranja elektroničkim potpisom - ne može služiti kao dokazno sredstvo pred sudom, odnosno ugovor sklopljen putem Interneta ne može pred sudom biti dokazan. Zato je potrebno primijeniti druga prikladnija dokazna sredstva za očitovanja volje putem Interneta.

Ispisom ili pohranjivanjem na disketu prikazano je stanje samo u određenom trenutku, što također predstavlja manjkav dokaz. Protokol o poslanim i primljenim e-mail-ovima je također nedostatan, jer su tehničke manipulacije relativno lako provedive. Zbog toga izjave preko e-maila za sada imaju samo ograničenu dokaznu snagu, one podliježu slobodnoj ocjeni dokaza, što znači da sudac prema osobnom nahođenju (pravo diskrecijske ocjene) odlučuje o njihovoj dokaznoj vrijednosti.

U praksi se iz tog razloga često događa, da mnogi ponuditelji potvrđuju svoje Internet narudžbe uobičajenim putem, posebno onda kad se radi o velikim iznosima ili kad se naručuju vrijedni proizvodi. Takva primjena uobičajene pošte kao rješenje ove dokazne problematike u proturječju je sa ulogom elektroničkog poslovanja, no ne mora biti zapreka daljnjem razvitku elektroničkog poslovanja kroz nove tehnologije.

Uostalom, cijeli niz kupoprodajnih odnosa, odvija se svakodnevno bez sklapanja pisanih ugovora. I kada kupujete novine na kiosku, vi ste pristupili sklapanju ugovora o prodaji. Pravno, ne postoje nikakve razlike između sklapanja ugovora o prodaji kilograma jabuka ili sklapanja ugovora o prodaji televizora.[10]

7.8. Evidencija davatelja usluga certificiranja u RH

Ministarstvo gospodarstva je nadležno za vođenje evidencije o davateljima usluga certificiranja. Evidencija davatelja usluga certificiranja je javna i vodi se u elektroničkom obliku. Hrvatski je zakon izjednačio valjanost domaćih certifikata, odnosno certifikata izdanih od strane certifikacijskih tijela sa sjedištem u Republici Hrvatskoj, i onih sa sjedištem u nekoj od zemalja članica Europske unije.

Što se valjanosti certifikata izdanih od strane certifikacijskih tijela sa sjedištem izvan Republike Hrvatske i Europske unije tiče, hrvatski zakon (sukladno odredbama europske Direktive) priznat će njihovu valjanost ako davatelj usluga certificiranja ispunjava uvjete za izdavanje kvalificiranih certifikata iz ZEP-a te je dobrovoljno akreditiran u Republici Hrvatskoj ili jednoj od zemalja članica Europske unije, ako neki domaći davatelj usluga certificiranja koji ispunjava uvjete za izdavanje kvalificiranih certifikata iz ovoga Zakona jamči za takve certifikate jednako kao da su njegovi, ako tako odredi bilateralni ili multilateralni sporazum između Republike Hrvatske i drugih zemalja ili međunarodnih organizacija te ako tako odredi bilateralni ili multilateralni sporazum između Europske unije i trećih zemalja ili međunarodnih organizacija.

[10] Ledinski,Stjepan,Sustavna programska potpora, Varaždin 2003
https://webcache.googleusercontent.com/search?q=cache:ApBD0sh0vekJ:https://documents.tips/documents/elektronicki-potpis.html+&cd=1&hl=hr&ct=clnk&gl=hr

8. Zakon o elektroničkoj ispravi

U općim odredbama Zakona o elektroničkoj ispravi (NN 150/2005) zakon uređuje pravo fizičkih i pravnih osoba na uporabu elektroničke isprave u svim poslovnim radnjama i djelatnostima te u postupcima koji se vode pred tijelima javne vlasti u kojima se elektronička oprema i programi mogu primjenjivati u izradi, prijenosu, pohrani i čuvanju informacija u elektroničkom obliku, pravna valjanost elektroničke isprave te uporaba i promet elektroničkih isprava.

Po čl.3 Zakona o elektroničkoj ispravi: Svaka fizička i pravna osoba svojom izričito očitovanom voljom prihvaća uporabu i promet elektroničkih isprava za svoje potrebe kao i za potrebe poslovnih i drugih odnosa s drugima, te fizička, odnosno pravna osoba koja je prihvatila uporabu i promet elektroničkih isprava, ne može odbiti elektroničku ispravu samo zbog toga što je sačinjena, korištena i prometovana u elektroničkom obliku.

Zakon o elektroničkom potpisu odluku je donio Hrvatski Sabor na temelju članka 88. Ustava Republike Hrvatske.

Po navedenom zakonu elektronički potpis znači napredan elektronički potpis utvrđen Zakonom o elektroničkom potpisu i kojim se pouzdano jamči identitet potpisnika i udovoljava zahtjevima sadržanim u članku 4. Zakona o elektroničkom potpisu.

Opće odredbe zakona o elektroničkom potpisu Članak 1. i Članak 2 navodim niže u tekstu:

Članak 1.

Ovim se Zakonom uređuje pravo fizičkih i pravnih osoba na uporabu elektroničkog potpisa u upravnim, sudskim i drugim postupcima, poslovnim i drugim radnjama, te prava, obveze i odgovornosti fizičkih i pravnih osoba u svezi s davanjem usluga certificiranja elektroničkog potpisa, ako posebnim zakonom nije drukčije određeno.

Članak 2.

Pojedini izrazi koji se rabe u ovom Zakonu imaju sljedeće značenje:

1. Elektronički potpis – znači skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju

potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta,

2. Napredan elektronički potpis – znači elektronički potpis koji pouzdano jamči identitet potpisnika i koji udovoljava zahtjevima sadržanim u članku 4. ovoga Zakona,

3. Potpisnik – znači osobu koja posjeduje sredstvo za izradu elektroničkog potpisa kojim se potpisuje, a koja djeluje u svoje ime ili u ime fizičke ili pravne osobe koju predstavlja,

4. Elektronički zapis – je cjelovit skup podataka koji su elektronički generirani, poslati, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju. Sadržaj elektroničkog zapisa uključuje sve oblike pisanog i drugog teksta, podatke, slike i crteže, karte, zvuk, glazbu, govor, računalne baze podataka,

5. Podaci za izradu elektroničkog potpisa – znače jedinstvene podatke, poput kodova ili privatnih kriptografskih ključeva, koje potpisnik koristi za izradu elektroničkog potpisa,

6. Sredstvo za izradu elektroničkog potpisa – znači odgovarajuću računalnu opremu ili računalni program koji potpisnik koristi pri izradi elektroničkog potpisa,

7. Sredstvo za izradu naprednoga elektroničkog potpisa – znači sredstvo za izradu potpisa koje udovoljava zahtjevima iz članka 9. ovoga Zakona,

8. Podaci za verificiranje elektroničkog potpisa – znače podatke poput kodova ili javnih kriptografskih ključeva koji se koriste u svrhu verificiranja (ovjere) elektroničkog potpisa,

9. Sredstvo za verificiranje potpisa – znači odgovarajuću računalnu opremu ili računalni program koji se koristi za primjenu podataka za verificiranje potpisa,

10. Certifikat – znači potvrdu u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom i potvrđuje identitet te osobe

11. Kvalificirani certifikat – znači certifikat koji udovoljava zahtjevima iz članka 11. ovoga Zakona i kojeg izdaje davatelj usluga izdavanja kvalificiranog certifikata koji ispunjava uvjete iz članka 17. ovoga Zakona,

12. Davatelj usluga certificiranja – znači pravnu ili fizičku osobu koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima,

13. Sredstvo za elektronički potpis – znači računalnu opremu ili računalni program ili njihove relevantne sastojke koji su namijenjeni za primjenu od strane davatelja usluga certificiranja za davanje usluga u vezi s elektroničkim potpisima ili su namijenjeni za primjenu kod izrade ili verificiranja elektroničkih potpisa.

9. Elektronički potpis i pravila EU

Pravila EU-a o elektroničkim potpisima, pečatima, vremenskim žigovima, uslugama elektroničke dostave i autentifikaciji na internetskim stranicama te o elektroničkim dokumentima utvrđena u Uredbi o eIDAS-u (Uredba o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu) izravno će se primjenjivati u svim državama članicama. (**12)**

To znači da će se, primjerice, elektronički potpis diljem EU-a priznavati jednako kao i onaj napisan rukom i da će biti jednako pravno valjan.

Građani poduzeća i javne uprave diljem EU-a mogu od 1. srpnja obavljati pogodne, sigurne i zakonski valjane prekogranične elektroničke transakcije, donosi Predstavništvo Europske komisije u Zagrebu.

9.1. E potpisi u EU-u

Utvrđuje se pravni okvir na europskoj razini za elektroničke potpise (e-Potpisi) te se priznaju davatelji usluga certificiranja. Njihov cilj je podijeljen u dvije stavke, a to su:

1. Pojednostavniti uporabu e-Potpisa
2. Pomoći im da postanu pravno priznati u svim zemljama EU-a

S ciljem osiguravanja ispravnog funkcioniranja unutarnjeg tržišta, istodobno težeći primjerenoj razini sigurnosti sredstava elektroničke identifikacije i usluga povjerenja, ovom se Uredbom:

a) utvrđuju uvjeti pod kojima države članice priznaju sredstva elektroničke identifikacije fizičkih i pravnih osoba koja su obuhvaćena prijavljenim sustavom elektroničke identifikacije druge države članice;

(b) utvrđuju pravila za usluge povjerenja, posebno za elektroničke transakcije; i

(c) uspostavlja pravni okvir za elektroničke potpise, elektroničke pečate, elektroničke vremenske žigove, elektroničke dokumente, usluge elektroničke preporučene dostave i usluge certificiranja za autentikaciju mrežnih stranica.

Uredba EU o Elektroničkom potpisu 910/2014 se primjenjuje na sustave elektroničke identifikacije koje je prijavila država članica, kao i na pružatelje usluga povjerenja koji imaju poslovni nastan u Uniji.

Ova se Uredba ne primjenjuje na pružanje usluga povjerenja koje se isključivo koriste unutar zatvorenih sustava koji proizlaze iz nacionalnog prava ili iz sporazumâ među utvrđenom skupinom sudionika i ne utječe na nacionalno pravo ili pravo Unije koje se odnosi na sklapanje i valjanost ugovorâ ili drugih pravnih ili postupovnih obveza u pogledu forme.

Navedenom direktivom definiraju se nove ideje:

1. elektronički potpis nam označuje podatke u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje;

2. Napredan elektronički potpis mora ispunjavati sljedeće zahtjeve:

(a) na nedvojben način je povezan s potpisnikom;

(b) omogućava identificiranje potpisnika;

(c) izrađen je korištenjem podacima za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom;

(d) povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka.

3. kvalificirani certifikat koji posebice mora obuhvaćati

a. naznaku da se izdaje kao kvalificirani certifikat

b. identifikaciju davatelja usluga certificiranja

c. ime potpisnika

d. mogućnost uvođenja specifičnog dodatnog elementa ovjere, poput datuma rođenja, potpisnika (ovisno o svrsi za koju je certifikat namijenjen)

e. podatke o verifikaciji potpisa: moraju odgovarati podacima o izradi potpisa koji su pod kontrolom potpisnika

f. datume početka i kraja razdoblja valjanosti certifikata

g. identifikacijsku oznaku certifikata

h. napredni elektronički potpis davatelja usluga certificiranja koji izdaje taj certifikat

Certifikat mora izdati davatelj usluga certificiranja koji zadovoljava specifične zahtjeve utvrđene u Uredbi.

U čl. 28. Kvalificiranog certifikata za elektroničke potpise u Službenog lista Europske unije u odredbama, certifikati za elektroničke potpise moraju ispunjavati zahtjeve utvrđene u Prilogu I., te ne smiju podlijegati obveznim zahtjevima koji prelaze zahtjeve utvrđene u Prilogu I.

Kvalificirani certifikati za elektroničke potpise mogu uključivati dodatna posebna obilježja koja nisu obvezna. Ta obilježja ne utječu na interoperabilnost i priznavanje kvalificiranih elektroničkih potpisa. No ako je kvalificirani certifikat za elektroničke potpise opozvan nakon početne aktivacije, on gubi valjanost od trenutka opoziva i njegov se status ni u kojem slučaju ne može vratiti u prijašnje stanje.

9.2. Pristup tržištu EU

Zemlje EU-a ne smiju isporučivati usluge certificiranja koje podliježu dobivanju prethodnog odobrenja bilo koje vrste.

Zemlje EU-a mogu imati vlastite sheme poticanja certifikacije poboljšanih značajki. Ne mogu ograničavati broj ovlaštenih davatelja usluga certificiranja. Također ne mogu ograničavati opskrbu uslugama certificiranja iz druge zemlje EU-a.

Zemlje EU-a mogu učiniti uporabu elektroničkih potpisa u javnome sektoru podložnom potencijalnim dodatnim zahtjevima. Ti zahtjevi moraju biti objektivni, transparentni, razmjerni i ne diskriminirajući.

9.3. Pravni učinci u EU

Napredni e-Potpis koji se zasniva na kvalificiranom certifikatu udovoljava pravnim zahtjevima potpisa u odnosu na podatke u elektroničkom obliku na isti način na koji vlastoručni potpis udovoljava tim zahtjevima u odnosu na podatke u pisanom obliku. [Iz

praktičnih razloga, ova se vrsta potpisa može zvati „kvalificiranim e-Potpisom”. Dopušten je kao dokaz u sudskim postupcima.

E-potpis ne može se pravno odbiti kao dokaz u sudskim postupcima isključivo na temelju toga što je:

- u elektroničkom obliku
- nije izrađen uporabom sigurnog sredstva za izradu potpisa

9.4. Zemlje članice EU

Zemlje članice moraju osigurati da davatelj usluga certificiranja koji izdaje kvalificirani certifikat preuzme određene obveze. One uključuju odgovornost za štetu prouzročenu bilo kojoj osobi ili subjektu, koji se u razumnoj mjeri oslanjaju o tom certifikatu:

- u vezi s točnošću svih podataka sadržanih u kvalificiranom certifikatu u vrijeme izdavanja
- u vezi s činjenicom da certifikat sadržava sve detalje propisane za kvalificirani certifikat u vrijeme izdavanja te da je potpisnik identificiran u certifikatu osoba kojoj je on izdan

Davatelj usluga certificiranja može naznačiti granicu vrijednosti transakcija za koje se certifikat može koristiti. Ta granica mora biti vidljiva trećim stranama. Davatelj ne smije biti odgovoran za štetu prouzrokovanu uporabom kvalificiranog certifikata koji prekoračuje utvrđena ograničenja.

Zemlje EU-a moraju osigurati uzajamno pravno priznavanje kvalificiranih certifikata i e-Potpisa iz zemalja koje nisu članice EU-a. Moraju biti ispunjeni određeni uvjeti o pouzdanosti kao što su:

- davatelji koji nisu iz EU-a moraju ispunjavati uvjete utvrđene ove Uredbe te biti ovlašteni prema programu dragovoljnog ovlašćivanja utvrđenog u zemlji EU-a; ili
- davatelj iz EU-a koji ispunjava uvjete utvrđene ovom Uredbom može jamčiti za certifikate davatelja koji nisu iz EU-a u jednakoj mjeri kao i za vlastite certifikate

Europska komisija može donijeti prijedloge kako bi se osigurala potpuna provedba međunarodnih standarda i sporazuma.

9.5. Zaštita podataka EU

Zemlje EU-a moraju osigurati da davatelji usluga certificiranja i nacionalna tijela odgovorna za ovlašćivanje ili nadzor udovoljavaju Direktivi 95/46/EZ o zaštiti osobnih podataka.

Donesena nova Uredba o elektroničkoj identifikaciji i uslugama povjerenja (eIDAS)

Uredba eIDAS (Uredba (EU) br. 910/2014) donesena je 2014. godine. Na snagu je stupila 17.9.2014., a primjenjivat će se od 1.7.2016., osim određenih članaka navedenih u članku 52. te Uredbe. Uredba (EU) br. 910/2014 od 30.6.2016. stavlja izvan snage Direktivu 1999/93/EZ.

10. EU potpis u Hrvatskoj u usporedbi sa EU

U Hrvatskoj se trenutačno na dva kolosijeka traže rješenja za problem dodatne birokratizacije računa, gdje se od početka godine prisiljava tvrtke da printaju, ručno potpisuju i pečate račune koje su primili e-mailom te ih se traži da izmisle novo radno mjesto "likvidatora računa" i time plate dodatan, birokratski trošak, čini se da će taj problem 1. srpnja riješiti Europska unija. Tada, naime, na snagu stupa "eIdas Uredba EU o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu". Njome će hrvatske i druge tvrtke u Uniji dobiti mogućnost stavljanja elektroničkog pečata na sve svoje dokumente koje imaju na računalima, poput ponuda, ugovora, pravilnika, ali i ulaznih računa. Svi takvi e-dokumenti time automatski postaju pravno valjani na cijelom teritoriju Unije pa tako i Hrvatskoj.

"Elektroničkom pečatu se kao dokazu u sudskim postupcima ne smije uskratiti pravni učinak i dopuštenost samo zbog toga što je on u elektroničkom obliku ili zbog toga što ne ispunjava sve zahtjeve za kvalificirani elektronički pečat", piše u eIdas Uredbi. Usto, kako neslužbeno doznajemo, paralelno ministar gospodarstva Tomislav Panenić pokušava kroz razgovor s ministrom financija Zdravkom Marićem pronaći još jedno rješenje za "likvidatore računa".

Trudi se ishoditi novu izmjenu Zakona o računovodstvu kojom bi se poništile odredbe tog zakona koje su stupile na snagu početkom ove godine. No, iz izvora bliskih Vladi doznajemo da je ta inicijativa zasad u početnoj fazi. Prva je na problem likvidacije ulaznih računa sredinom veljače ukazala Udruga nezavisnih hrvatskih izvoznika softvera CISEx. Ona je procijenila da će samo hrvatske IT tvrtke ta nova birokratska obveza godišnje stajati šest milijuna kuna. "Procjenjujemo da se u jednoj prosječnoj IT tvrtki koja ima 30 zaposlenika i oko sto ulaznih računa mjesečno na taj posao potroši 500 minuta, odnosno 8 sati", navodi CISEx. Koliki je pak trošak likvidacije računa na razini cijelog gospodarstva teško je procijeniti. Matija Matečić, osnivač servisa za izdavanje računa Solo, kaže da se očito prilikom izmjena Zakona o računovodstvu mislilo mahom o velikim poslovnim sustavima.

"To su, izgleda, oni gdje po desetak i više ljudi piše i prima račune, pa im treba kontrolor, ali mikro, mali i srednji poduzetnici nemaju takvih problema, jer kod njih takve poslove u pravilu

obavlja direktor", kaže Matečić. Država je pak, prije nego što je EU nametnula elektronički pečat, osmislila i alternativu – propisala je format e-računa koji priznaje Porezna uprava. Amera Zulić Vrabec iz HUP ICT-a kaže da od 1. ožujka ministarstva moraju primati e-račune, odnosno ne mogu ih odbijati. "Jednako kao što je APIS IT postao središnja točka u fiskalizaciji, tako je za pitanje e-računa u državi središnja točka Fina, koja zaprima i dalje prosljeđuje e-račune prema ministarstvima", pojašnjava Zulić Vrabec.

Dodaje da je sustav zaživio i u gospodarstvu u Agrokoru i Ini. Kako neslužbeno doznajemo, e-račune za Agrokor obrađuje mStart. Njihova razmjena definirana je ugovorom i točno definiranim formatom e-računa, a pohranjuju se na specijalne poslužitelje s obzirom na to da se računi moraju arhivirati određeni broj godina. "U Hrvatskoj, za razliku od Slovenije, nije posebno propisano da se takve arhive moraju certificirati, već svatko radi svoje rješenje", kaže Zulić Vrabec. Mladen Amidžić, predsjednik Uprave Trilixa, objašnjava pak da se time rješava pitanje arhive računa, ali ne i ostalih dokumenata. Ističa da ne postoji razlog zašto bi tvrtka koja ima ERP koristila papir. "Dobra reforma bi bila kada bi država napokon omogućila korištenje elektroničkog pečata i kad bi se odlučila koji model nadzora nad digitalnim arhivama želi", zaključuje Amidžić, koji navodi da u Sloveniji državna agencija certificira digitalne arhive te je na taj način otvorila cijelu jednu novu poslovnu nišu.

11. Hrvatski Zakon o elektroničkoj ispravi

Strukturno sastojeći se od triju glavnih dijelova, općih odredaba, definicije elektroničke isprave i odredaba vezanih za njezino stavljanje u promet, Zakon načelno određuje da elektronička isprava ima istu pravnu snagu kao i ona izdana na papiru, osim u slučaju da se drugim zakonima izričito traži isprava na papiru. Mnogi hrvatski zakoni izričito spominju papirnate isprave, a tek neki u posljednje vrijeme dopunjeni ili doneseni tehnološki neutralno (bez posebne oznake) podrazumijevaju izdavanje elektroničke isprave ili izričito dopuštaju da se ona izda i u elektroničkom obliku.

Zakon daje dvojaku definiciju elektroničke isprave, pa bi se moglo izdvojiti definiciju elektroničke isprave u širem smislu, kao jednoznačno povezan cjelovit skup podataka koji su elektronički oblikovani (izrađeni s pomoću računala i drugih elektroničkih uređaja), poslani, primljeni ili sačuvani na nekom (elektroničkom, magnetnom, optičkom ili drugom) mediju i koji sadržavaju svojstva kojima se utvrđuje izvor (stvaratelj), utvrđuje vjerodostojnost sadržaja te dokazuje postojanost sadržaja u vremenu.

Hrvatski je zakonodavac u hrvatski pravni sustav uveo elektronički potpis sukladno recentnoj komparativno pravnoj praksi. Suvremeni okvir zakonske regulacije elektroničkog potpisa počinje usvajanjem europske Direktive o elektroničkom potpisu 1999. godine, koja je u pravnu teoriju uvela razlikovanje između osnovnog elektroničkog potpisa i njegova kvalificiranog oblika, naprednog elektroničkog potpisa.

11.1 Pod zakonski propisi

Pod zakonski propis sadrži nekoliko pravilnika koji su izdani od strane Narodnih novina, te se od tada koriste, te do izdavanja novog pravilnika, dopuna ili izmjenama su važeći, te ih se u potpunosti treba pridržavati.

- Pravilnik o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN107/10, 89/13)
- Pravilnik o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj (NN 107/10)

- Pravilnik o službenoj iskaznici inspektora za nadzor davatelja usluga certificiranja (NN 109/11)
- Popis normizacijskih dokumenata u području primjene Zakona o elektroničkom potpisu i Pravilnika o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata NN 89/13
- Uredba o djelokrugu , sadržaju i nositelju poslova certificiranja elektroničkih potpisa za tijela državne uprave, NN 146/04

12. Zaključak

Kako živimo u naprednom dobu, u dobu tehnologije elektronički potpis za nas je svakodnevica. Bilo da se radi o digitalnom potpisu, ili o skeniranom potpisu, on nam je jedini izvor kako biti u skladu sa tehnologijom i kako si pojednostaviti poslovanje.

Mnoge institucije danas umjesto ručnog potpisa koriste digitalni potpis, koji ima istu važnost, te je pravno u potpunost potkrijepljeno. Iako svi znamo da imamo pravnu zaštitu , mnogi ljudi se boje digitalnog potpisa, jer su uvjereni da se njihov potpis može iskoristiti u bilo koje druge svrhe. Za takve slučajeve imamo zaštitu koja je regulirana zakonom.

Osim dva najčešće korištena potpisa, postoji biometrijski potpis, koji se temelji na DNK, mrežnici oka, otisku prsta.. najmanje je zastupljen, pogotovo u nerazvijenim državama, ali definitivno 100% točan, i ne postoji mogućnost krađe podataka.

Za sada tržište nije u potpunosti doraslo da se potpuno okrene elektronskom potpisu, što iz neopremljenosti i nedostatak sredstava, što zbog manjka stručnosti, no međutim svakako je vidljivo da će u budućnosti biti zastupljen u većem omjeru nego danas.

Andela Tomić

LITERATURA

1. Dujella, Andrej, Marcel Maretić, Kriptografija, Element Zagreb 2007
2. Housley, Russ, Tim Polk, 2001. Planning for PKI, Wiley Computer Publishing, Canada
3. Katulić, Tihomir: Razvoj pravne regulacije elektroničkog potpisa, elektroničkog certifikata,
4. Krnić, Ivan, Zoran Regvart, Interna Skripta, PKI i Java programiranje za PKI
5. Ledinski, Stjepan, Sustavna programska potpora, Varaždin 2003

Pravni izvori

Zakon o elektroničkom potpisu NN 10/02, 80/08, 30/14
Zakon o elektroničkoj ispravi NN 150/2005
Zakon o osobnoj iskaznici NN 11/2002, 62/15
Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ
Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ

Web izvori:

MINGO, Ministarstvo gospodarstva https://www.mingo.hr/page/kategorija/e-potpis

INDEKS, Elektronički potpis u EU, valjanost, http://www.index.hr/vijesti/clanak/od-sutra-diljem-eua-elektronicki-potpisi-i-pecati-postaju-jednako-valjani-kao-oni-fizicki/903309.aspx

Poslovni Dnevnik, EU uvodielektroničkipečatispašavamilijunetvrtkama", http://www.poslovni.hr/hrvatska/eu-uvodi-elektronicki-pecat-i-spasava-milijune-tvrtkama-311184

FINA web, Elektroničkipotpishttp://www.fina.hr/Default.aspx?art=10737